careful review, and has added claims 27-30, which correspond directly to the subject matter of claims 15 and 16. The Applicant respectfully requests that these claims be allowed.

III. Rejections under 35 U.S.C. § 102

The Examiner rejected claim 24 as being anticipated by U.S. Patent No. 5,774, 548, issued to Bando *et al.* ("Bando") under 35 U.S.C. § 102(b). This rejection is respectfully traversed.

The Applicant's invention relates to a method and apparatus for transmitting an encrypted data stream. More specifically, the Applicant's invention provides a secure decoder configuration which is resistant to attempts to de-encrypt data during a given transmission. Typically, in conventional systems, scrambled data is transmitted together with a control word capable of descrambling the data. The control word is encrypted by an "exploitation" key and is transmitted in an encrypted form. The scrambled data and the encrypted control word are then received by a decoder having an equivalent of the exploitation key stored on a smart card inserted into the decoder. The decoder can then decrypt the control word and descramble the data. The Applicant's invention, as recited in the claims, incorporates a portable security module that descrambles the data and encrypts the descrambled data before sending the data to the decoder.

The Examiner rejected claim 24, stating that "Bando et al. discloses these features (see at least the abstract)." The Applicant respectfully disagrees. Bando discloses an arrangement to automatically change between a scrambled digital data output and descrambled digital data output of a receiver. The arrangement makes use of a control signal inserted into the transmission signal conforming to a program provider's policy. Abstract, lines 1-4. Bando,

however, fails to disclose sending a scrambled data stream from a decoder to a portable security module inserted into the decoder as recited in claim 24. Instead, in Bando, a scrambled data stream is sent to a descrambler. Notably, Bando does not disclose encrypting the data stream after descrambling. The Applicant's invention, advantageously, increases the overall security of the system, as is described on pages 5-7 of the Specification.

The Applicant believes that Bando may not be used as a basis for rejecting claim 24 under 35 U.S.C. § 102 because Bando does not disclose all of the claimed features of the present invention. For example, Bando does not disclose sending a scrambled data stream to a portable security module inserted in the decoder as explained above. Thus, Bando does not disclose *each and every element* of the claimed invention and, as a result, withdrawal of the rejection is respectfully requested.

Furthermore, there is no disclosure in Bando which suggests modifying Bando to obtain the Applicant's invention and, thus, the Applicant believes that Bando may not serve as the basis for a § 103 rejection for the reasons discussed below.

IV. Rejections under 35 U.S.C. § 103

The Examiner rejected claims 2-5, 14, 17, and 25 under 35 U.S.C. § 103 stating "[i]t would have been obvious to anyone having an ordinary level of skill in the art at the time the invention was made to have used a key and the various components of these claims . . . ." The Applicant respectfully disagrees with the Examiner's assertion. The Applicant acknowledges that some specific features of the claims may be known in the art of data transmission between network nodes. However, the individual knowledge of these elements does not render the claims of the present invention obvious. For example, claim 3, which depends from claim 24, recites a

B

limitation of "encrypting the data stream in the security module using a first encryption key" that depends on a decoder identity value. The Examiner has neither cited prior art in support of the § 103 rejection, nor given any reasoning as to why this specific limitation is obvious in view of prior art. Thus, the Applicant believes these rejections to be improper omnibus rejections, and respectfully requests that the Examiner either cite prior art disclosing the specific claimed features or provide an affidavit of personal knowledge pursuant to 37 C.F.R. § 1.104 (d)(2).

In the absence of any such prior art, the Applicant believes that Bando, as explained above, does not render obvious the claimed invention. Bando fails to disclose or suggest sending a scrambled data stream from a decoder to a portable security module inserted into the decoder as recited in claim 24. Claims 2-14, 17, 19-21 and 25 all depend, either directly or indirectly, from claim 24. Therefore, combining Bando with the knowledge of one skilled in the art does not render the claims obvious.

The Examiner rejected claims 6-10 and 12-13 as being obvious over Bando in view of a publication entitled "Applied Cryptography" by Schneier. Claims 7-10 and 12-13 all depend from claim 6, either directly or indirectly. Claim 6 requires that the data stream by encrypted ***in*** the security module by a first encryption key dependent on a random or pseudo-random number. Neither Bando nor Schneier disclose or suggest encrypting a descrambled signal ***in*** a security module. Rather, both Bando and Schneier use the security module simply to transport and deliver a key. Thus, claim 6 is patentable over the cited prior art. Claims 7-10 and 12-13, which depend from claim 6, are likewise patentable.

The Examiner rejected claim 11 as being obvious over Bando in view of the knowledge of one skilled in the art. The Applicant respectfully disagrees with this rejection. Claim 11 also depends from claim 6, and thus is patentable over the combination of Bando and

B

Schneier for the reasons discussed above. Furthermore, the Examiner has neither cited prior art, nor provided any reasoning as to why this specific limitation is obvious in view of the prior art. Thus, the Applicant believes these rejections to be improper omnibus rejections and respectfully requests that the Examiner either cite prior art disclosing the specific claimed features or provide an affidavit of personal knowledge pursuant to 37 C.F.R. § 1.104 (d)(2). The Applicant believes claim 11 to be allowable over the cited prior art for the reasons discussed above.

The Applicant believes this paper to be responsive to each ground raised by the Examiner in his Office Action of November 8, 2000. The Applicant further believes that the application is now in condition for allowance and respectfully requests favorable action in the form of a Notice of Allowance.

Please apply any charges not covered, or any credits, to Deposit Account 50-0591 (Reference Number 11345.009001).

Respectfully submitted,

Date: 2/8/01

Jonathan P. Osha, Reg. No. 33,986
Rosenthal & Osha L.L.P.
700 Louisiana, Suite 4550
Houston, TX 77002

Telephone: (713) 228-8600
Facsimile: (713) 228-8778

14258_1.DOC

B